Abstract

A system, computerized method and computer-readable medium are provided for the detection of an operating system exploitation, such as a rootkit install. The operating system is monitored to ascertain an occurrence of anomalous activity resulting from operating system behavior which deviates from any one of a set of pre-determined operating system parameters. Each parameter corresponds to a dynamic characteristic associated with an unexploited operating system. Output can then be generated to indicate any anomalous activity that is ascertained. The computer-readable medium may comprise a loadable kernel module for detecting hidden patches, processes, files or other kernel modules.